

revolving cylinders with  
clean, full flavored an

...ed from  
...ing.

# Tabla de contenido

1. Monta y configura el entorno de prueba anterior y realiza pruebas a nivel de red de que las máquinas se comunican entre sí. ....	3
Kali Linux.....	4
prueba de comunicación .....	4
Ubuntu Server (Router) .....	5
Windows 10 .....	6
prueba de comunicación .....	9
2. Realiza pruebas necesarias para poder obtener una conclusión de cuándo un FW está presente en un servidor. Para ello puedes enviar paquetes de tipo ACK mal formados e ir completando la siguiente tabla en función del estado del firewall (activo, no activo) del router y del estado (activo, no activo) del servicio de conexión de escritorio remoto de la máquina Windows. Para la generación de paquetes ACK mal formados utiliza las siguientes herramientas vistas en clase: nmap y hping3. Anota la/s conclusiones que obtienes.....	11
3. Vuelve a realizar las pruebas anteriores, pero desactivando el FW del router Ubuntu Server y activando una regla de filtrado en la máquina Windows para todos los paquetes TCP correspondientes a una conexión con el escritorio remoto. Completa la con los resultados obtenidos y anota las conclusiones que obtienes.....	12
Creación de la regla .....	12
4. Como habrás comprobado por las pruebas realizadas, a través de la generación y envío de paquetes ACK mal formados se puede llegar a inferir la existencia de un firewall. Configura iptables en el router Ubuntu Server para que filtre los paquetes de tipo ACK mal formados y no se pueda realizar el fingerprinting para la detección de un firewall. Para ello puedes consultar las "Extensiones TCP" de la web de NetFilter.....	16

# Tabla de ilustraciones

Ilustración 1 Red NAT.....	3
Ilustración 2 Esquema de red .....	3
Ilustración 3 Fichero de configuración /etc/network/interfaces.....	4
Ilustración 4 Pruebas de comunicación .....	4
Ilustración 5 Fichero de configuración de /etc/netplan/00-installer-config.yaml .....	5
Ilustración 6 Pruebas de comunicación .....	5
Ilustración 7 Pruebas de comunicación .....	5
Ilustración 8 Panel de control .....	6
Ilustración 9 Redes e Internet .....	6
Ilustración 10 Centro de redes y recursos compartidos .....	7
Ilustración 11 Cambiar configuración del adaptador.....	7
Ilustración 12 Seleccionamos interfaz .....	8
Ilustración 13 Propiedades .....	8
Ilustración 14 Asignación de IP .....	9
Ilustración 15 Prueba de comunicación.....	9
Ilustración 16 Prueba de comunicación.....	10
Ilustración 17 Regla de entrada 1 .....	12
Ilustración 18 Regla de entrada 2 .....	12
Ilustración 19 Regla de entrada 3 .....	13
Ilustración 20 Regla de entrada 4 .....	13
Ilustración 21 Regla de entrada 5 .....	14
Ilustración 22 Regla de entrada 6 .....	14
Ilustración 23 Regla iptables.....	16
Ilustración 24 Regla iptables.....	16
Ilustración 25 Regla iptables.....	17
Ilustración 26 Regla iptables.....	17

1. MONTA Y CONFIGURA EL ENTORNO DE PRUEBA ANTERIOR Y REALIZA PRUEBAS A NIVEL DE RED DE QUE LAS MÁQUINAS SE COMUNICAN ENTRE SÍ.

Para esta práctica he creado una red interna llamada "2.0.0.0/8" y una red NAT llamada "t c p":

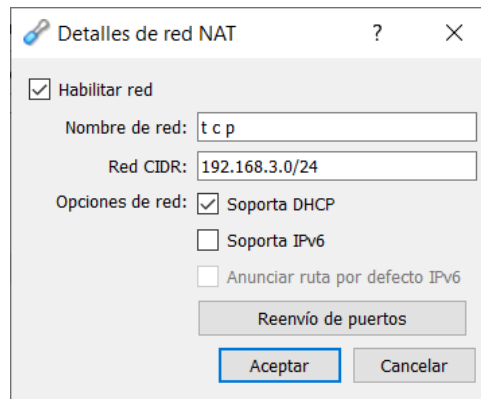


Ilustración 1 Red NAT

He seguido este esquema de red:

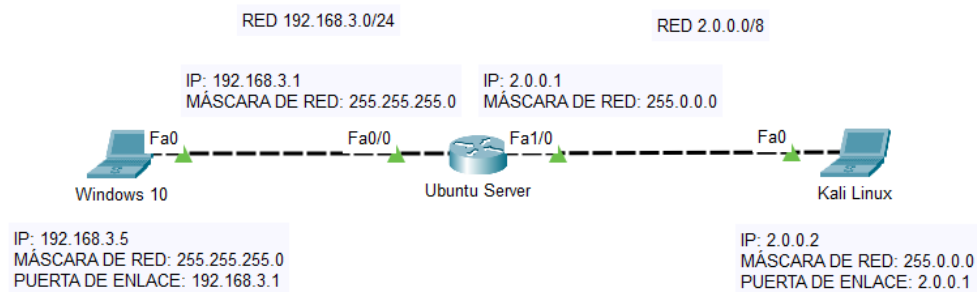


Ilustración 2 Esquema de red

Nos dirigimos a “/etc/network/interfaces” y lo modificamos con la siguiente configuración:

```
GNU nano 4.9.3 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
    address 2.0.0.2
    netmask 255.0.0.0
    gateway 2.0.0.1
```

Ilustración 3 Fichero de configuración /etc/network/interfaces

## PRUEBA DE COMUNICACIÓN

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 2.0.0.2 netmask 255.0.0.0 broadcast 2.255.255.255
    inet6 fe80::a00:27ff:fe6e:1c07 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:6e:1c:07 txqueuelen 1000 (Ethernet)
    RX packets 182 bytes 13546 (13.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 546 bytes 34711 (33.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 30 bytes 1660 (1.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 30 bytes 1660 (1.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# ping 2.0.0.2 -c 2
PING 2.0.0.2 (2.0.0.2) 56(84) bytes of data.
64 bytes from 2.0.0.2: icmp_seq=1 ttl=64 time=0.010 ms
64 bytes from 2.0.0.2: icmp_seq=2 ttl=64 time=0.030 ms

--- 2.0.0.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1013ms
rtt min/avg/max/mdev = 0.010/0.020/0.030/0.010 ms
root@kali:~# ping 2.0.0.1 -c 2
PING 2.0.0.1 (2.0.0.1) 56(84) bytes of data.
64 bytes from 2.0.0.1: icmp_seq=1 ttl=64 time=0.489 ms
64 bytes from 2.0.0.1: icmp_seq=2 ttl=64 time=0.546 ms

--- 2.0.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1024ms
rtt min/avg/max/mdev = 0.489/0.517/0.546/0.028 ms
root@kali:~# ping 192.168.3.1 -c 2
PING 192.168.3.1 (192.168.3.1) 56(84) bytes of data.
64 bytes from 192.168.3.1: icmp_seq=1 ttl=64 time=0.390 ms
64 bytes from 192.168.3.1: icmp_seq=2 ttl=64 time=0.376 ms

--- 192.168.3.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 0.376/0.383/0.390/0.007 ms
root@kali:~# ping 192.168.3.5 -c 2
PING 192.168.3.5 (192.168.3.5) 56(84) bytes of data.
64 bytes from 192.168.3.5: icmp_seq=1 ttl=127 time=0.723 ms
64 bytes from 192.168.3.5: icmp_seq=2 ttl=127 time=0.702 ms

--- 192.168.3.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1030ms
rtt min/avg/max/mdev = 0.702/0.712/0.723/0.010 ms
```

Ilustración 4 Pruebas de comunicación



## UBUNTU SERVER (ROUTER)

Para configurar nuestro Ubuntu Server introducimos "nano /etc/network/interfaces" e insertamos lo siguiente:

```
GNU nano 4.8 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.3.1/24]
    enp0s8:
      dhcp4: no
      addresses: [2.0.0.1/8]
  version: 2
```

Ilustración 5 Fichero de configuración de /etc/netplan/00-installer-config.yaml

```
root@planb:~# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.3.1 netmask 255.255.255.0 broadcast 192.168.3.255
    inet6 fe80::a00:27ff:fe1e:275c prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:1e:27:5c txqueuelen 1000 (Ethernet)
    RX packets 2279 bytes 170899 (170.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1357 bytes 120409 (120.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 2.0.0.1 netmask 255.0.0.0 broadcast 2.255.255.255
    inet6 fe80::a00:27ff:fe8e:5cd prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:8e:05:cd txqueuelen 1000 (Ethernet)
    RX packets 544 bytes 34623 (34.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 219 bytes 16476 (16.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 38388 bytes 2725960 (2.7 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 38388 bytes 2725960 (2.7 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Ilustración 6 Pruebas de comunicación

```
root@planb:~# ping 2.0.0.2 -c 2
PING 2.0.0.2 (2.0.0.2) 56(84) bytes of data.
64 bytes from 2.0.0.2: icmp_seq=1 ttl=64 time=0.357 ms
64 bytes from 2.0.0.2: icmp_seq=2 ttl=64 time=0.577 ms

--- 2.0.0.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1014ms
rtt min/avg/max/mdev = 0.357/0.467/0.577/0.110 ms
root@planb:~# ping 2.0.0.1 -c 2
PING 2.0.0.1 (2.0.0.1) 56(84) bytes of data.
64 bytes from 2.0.0.1: icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from 2.0.0.1: icmp_seq=2 ttl=64 time=0.030 ms

--- 2.0.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1012ms
rtt min/avg/max/mdev = 0.018/0.024/0.030/0.006 ms
root@planb:~# ping 192.168.3.1 -c 2
PING 192.168.3.1 (192.168.3.1) 56(84) bytes of data.
64 bytes from 192.168.3.1: icmp_seq=1 ttl=64 time=0.021 ms
64 bytes from 192.168.3.1: icmp_seq=2 ttl=64 time=0.047 ms

--- 192.168.3.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1013ms
rtt min/avg/max/mdev = 0.021/0.034/0.047/0.013 ms
root@planb:~# ping 192.168.3.5 -c 2
PING 192.168.3.5 (192.168.3.5) 56(84) bytes of data.
64 bytes from 192.168.3.5: icmp_seq=1 ttl=128 time=0.463 ms
64 bytes from 192.168.3.5: icmp_seq=2 ttl=128 time=0.668 ms

--- 192.168.3.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1014ms
rtt min/avg/max/mdev = 0.463/0.565/0.668/0.102 ms
```

Ilustración 7 Pruebas de comunicación

## WINDOWS 10

Nos dirigimos a Inicio e insertamos "Panel de control"

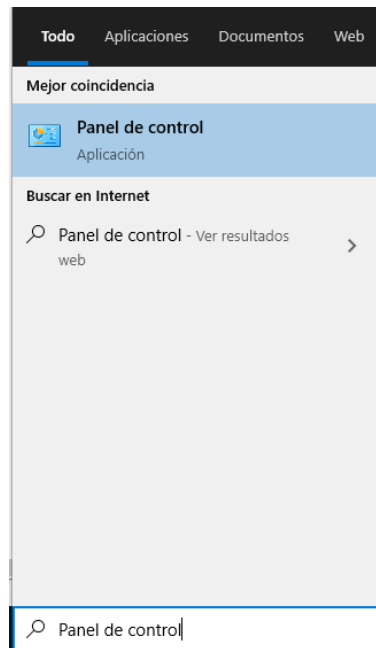


Ilustración 8 Panel de control

Seleccionamos "Redes e Internet"

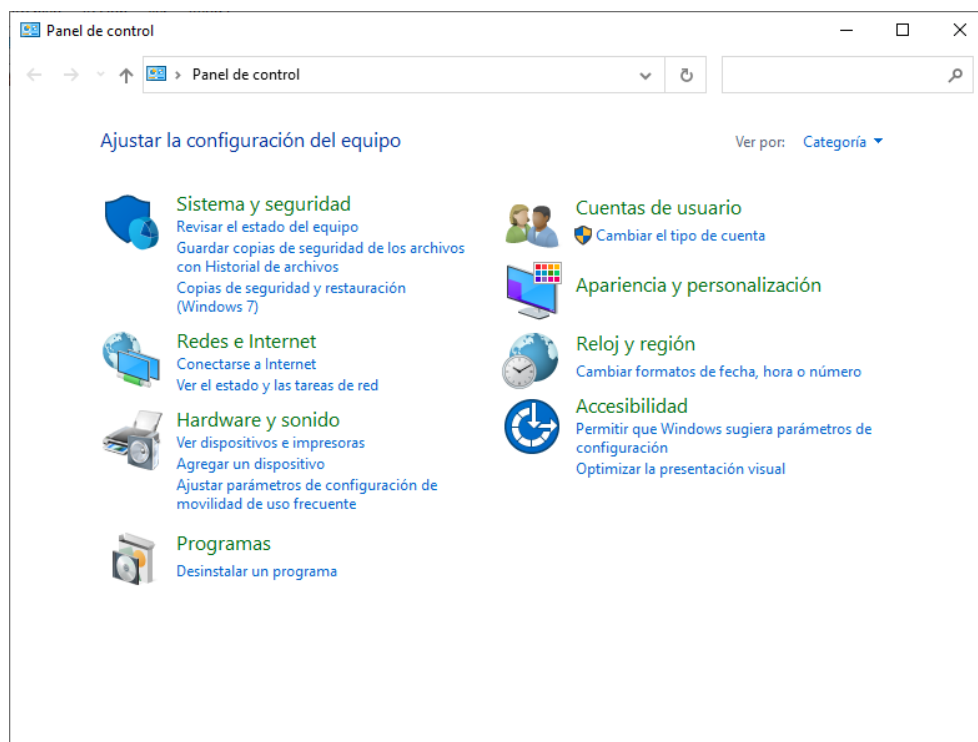


Ilustración 9 Redes e Internet

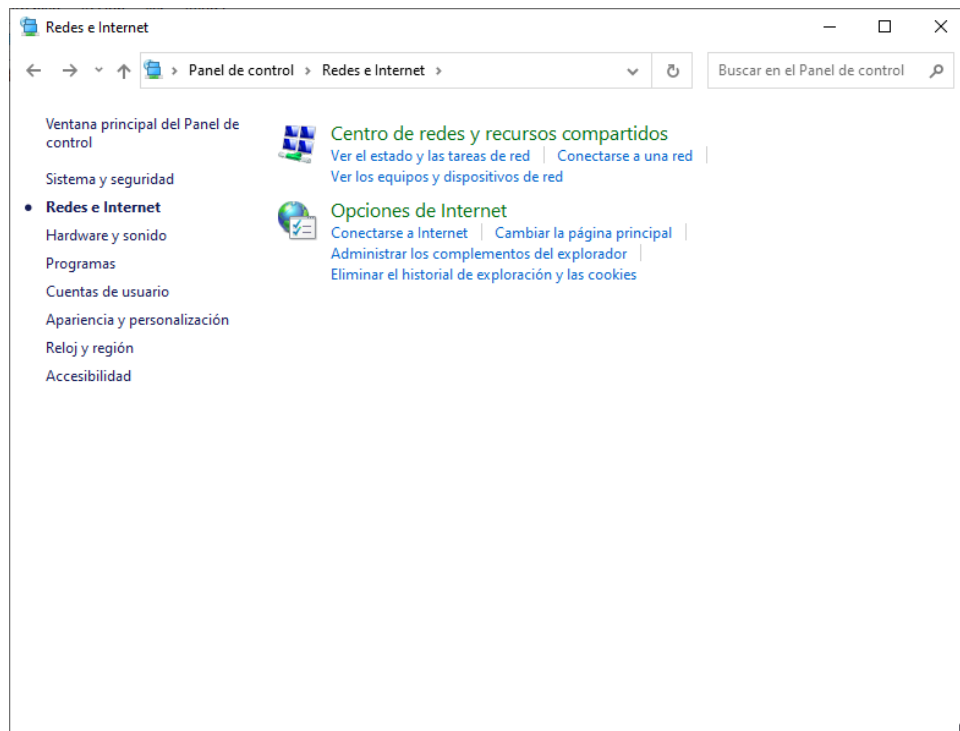


Ilustración 10 Centro de redes y recursos compartidos

Seleccionamos "Cambiar configuración del adaptador"

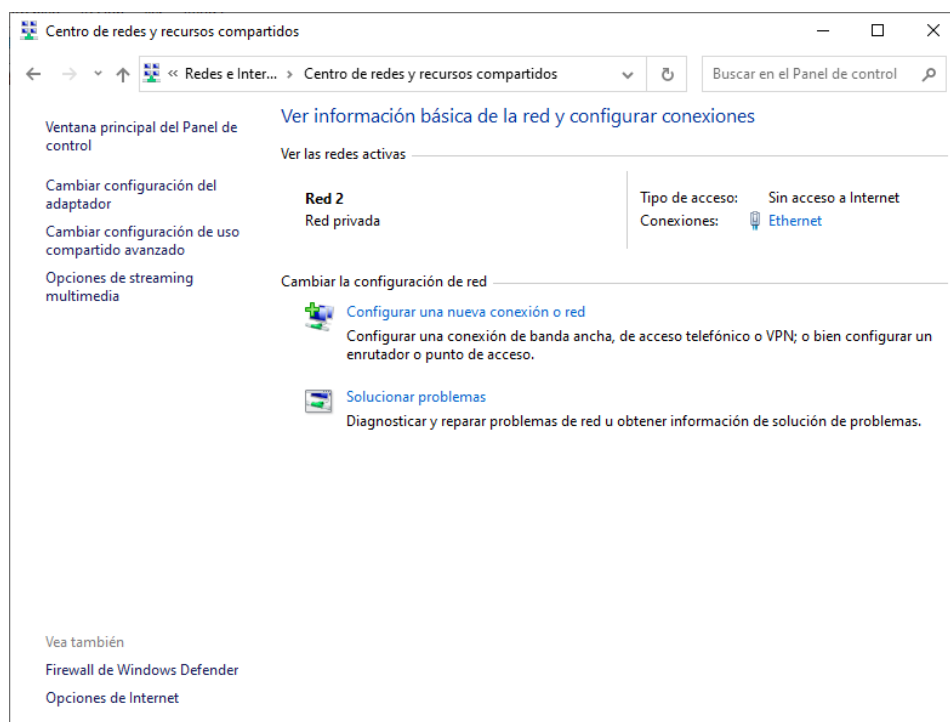


Ilustración 11 Cambiar configuración del adaptador



Seleccionamos nuestra interfaz de red y con el botón secundario del ratón seleccionamos "Propiedades"

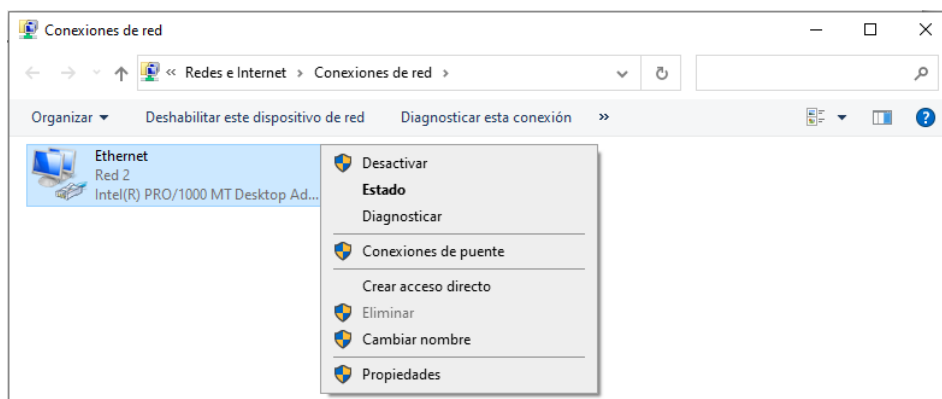


Ilustración 12 Seleccionamos interfaz

Seleccionamos "Protocolo de Internet versión 4 (TCP/IPv4)" > "Propiedades"

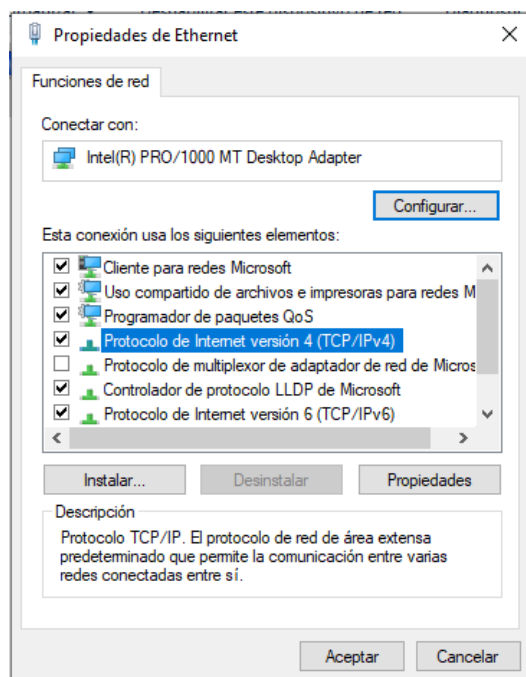


Ilustración 13 Propiedades

Asignamos la dirección IP que deseemos y el resto de parámetros

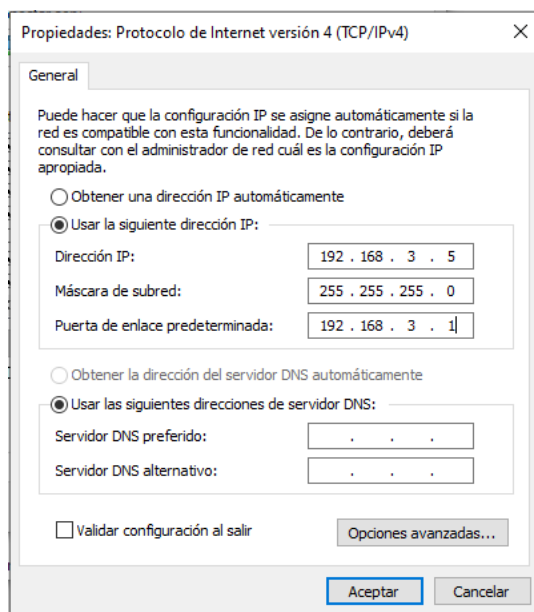


Ilustración 14 Asignación de IP

## PRUEBA DE COMUNICACIÓN

```
C:\Users\martha>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . : home
    Vínculo: dirección IPv6 local. . . : fe80::88db:2a3b:e31b:7a4%6
    Dirección IPv4. . . . . : 192.168.3.5
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.3.1

C:\Users\martha>ping 2.0.0.2 -n 2

Haciendo ping a 2.0.0.2 con 32 bytes de datos:
Respuesta desde 2.0.0.2: bytes=32 tiempo<1m TTL=63
Respuesta desde 2.0.0.2: bytes=32 tiempo=1ms TTL=63

Estadísticas de ping para 2.0.0.2:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\martha>ping 2.0.0.1 -n 2

Haciendo ping a 2.0.0.1 con 32 bytes de datos:
Respuesta desde 2.0.0.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 2.0.0.1: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 2.0.0.1:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Ilustración 15 Prueba de comunicación

```
C:\Users\martha>ping 192.168.3.1 -n 2

Haciendo ping a 192.168.3.1 con 32 bytes de datos:
Respuesta desde 192.168.3.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.3.1: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.3.1:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\martha>ping 192.168.3.5 -n 2

Haciendo ping a 192.168.3.5 con 32 bytes de datos:
Respuesta desde 192.168.3.5: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.3.5: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.3.5:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

*Ilustración 16 Prueba de comunicación*

2. REALIZA PRUEBAS NECESARIAS PARA PODER OBTENER UNA CONCLUSIÓN DE CUÁNDO UN FW ESTÁ PRESENTE EN UN SERVIDOR. PARA ELLO PUEDES ENVIAR PAQUETES DE TIPO ACK MAL FORMADOS E IR COMPLETANDO LA SIGUIENTE TABLA EN FUNCIÓN DEL ESTADO DEL FIREWALL (ACTIVO, NO ACTIVO) DEL ROUTER Y DEL ESTADO (ACTIVO, NO ACTIVO) DEL SERVICIO DE CONEXIÓN DE ESCRITORIO REMOTO DE LA MÁQUINA WINDOWS. PARA LA GENERACIÓN DE PAQUETES ACK MAL FORMADOS UTILIZA LAS SIGUIENTES HERRAMIENTAS VISTAS EN CLASE: NMAP Y HPING3. ANOTA LA/S CONCLUSIONES QUE OBTIENES.

FIREWALL	SERVICIO RDP 3389/TCP	nmap UNFILTERED	nmap FILTERED	hping RESPUESTA RESET (R), VOID
Desactivado	Desactivado	<pre>root@kali:~# nmap 192.168.3.5 -p 3389 -sA Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-22 17:44 CET Nmap scan report for 192.168.3.5 Host is up (0.00099s latency).  PORT      STATE      SERVICE 3389/tcp  unfiltered ms-wbt-server  Nmap done: 1 IP address (1 host up) scanned in 13.03 seconds</pre>		<pre>root@kali:~# hping3 192.168.3.5 -p 3389 -A HPING 192.168.3.5 (eth0 192.168.3.5): A set, 40 headers + 0 data bytes len=46 ip=192.168.3.5 ttl=127 DF id=13494 sport=3389 flags=R seq=6 win=0 rt t=2.8 ms len=46 ip=192.168.3.5 ttl=127 DF id=13495 sport=3389 flags=R seq=7 win=0 rt t=1.8 ms</pre>
Desactivado	Activado	<pre>root@kali:~# nmap 192.168.3.5 -p 3389 -sA Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-22 17:52 CET Nmap scan report for 192.168.3.5 Host is up (0.00097s latency).</pre>		<pre>root@kali:~# hping3 192.168.3.5 -p 3389 -A HPING 192.168.3.5 (eth0 192.168.3.5): A set, 40 headers + 0 data bytes len=46 ip=192.168.3.5 ttl=127 DF id=13503 sport=3389 flags=R seq=0 win=0 rt t=6.5 ms len=46 ip=192.168.3.5 ttl=127 DF id=13504 sport=3389 flags=R seq=1 win=0 rt t=3.8 ms len=46 ip=192.168.3.5 ttl=127 DF id=13505 sport=3389 flags=R seq=2 win=0 rt t=3.1 ms ^C --- 192.168.3.5 hping statistic --- 3 packets transmitted, 3 packets received, 0% packet loss round-trip min/avg/max = 3.1/4.5/6.5 ms</pre>
Activado	Desactivado		<pre>root@kali:~# nmap 192.168.3.5 -p 3389 -sA Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-22 18:02 CET Nmap scan report for 192.168.3.5 Host is up (0.0010s latency).  PORT      STATE      SERVICE 3389/tcp  filtered  ms-wbt-server  Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds</pre>	<pre>root@kali:~# hping3 192.168.3.5 -p 3389 -A HPING 192.168.3.5 (eth0 192.168.3.5): A set, 40 headers + 0 data bytes ^C --- 192.168.3.5 hping statistic --- 63 packets transmitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms</pre>
Activado	Activado		<pre>root@kali:~# nmap 192.168.3.5 -p 3389 -sA Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-22 18:05 CET Nmap scan report for 192.168.3.5 Host is up (0.00081s latency).  PORT      STATE      SERVICE 3389/tcp  filtered  ms-wbt-server  Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds</pre>	<pre>root@kali:~# hping3 192.168.3.5 -p 3389 -A HPING 192.168.3.5 (eth0 192.168.3.5): A set, 40 headers + 0 data bytes ^C --- 192.168.3.5 hping statistic --- 16 packets transmitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms</pre>

3. VUELVE A REALIZAR LAS PRUEBAS ANTERIORES, PERO DESACTIVANDO EL FW DEL ROUTER UBUNTU SERVER Y ACTIVANDO UNA REGLA DE FILTRADO EN LA MÁQUINA WINDOWS PARA TODOS LOS PAQUETES TCP CORRESPONDIENTES A UNA CONEXIÓN CON EL ESCRITORIO REMOTO. COMPLETA LA CON LOS RESULTADOS OBTENIDOS Y ANOTA LAS CONCLUSIONES QUE OBTIENES.

### CREACIÓN DE LA REGLA

Nos dirigimos a “Windows Defender Firewall con seguridad avanzada” y en la columna de la izquierda seleccionamos la opción “Reglas de entrada” y en la columna de la derecha “Nueva regla...”

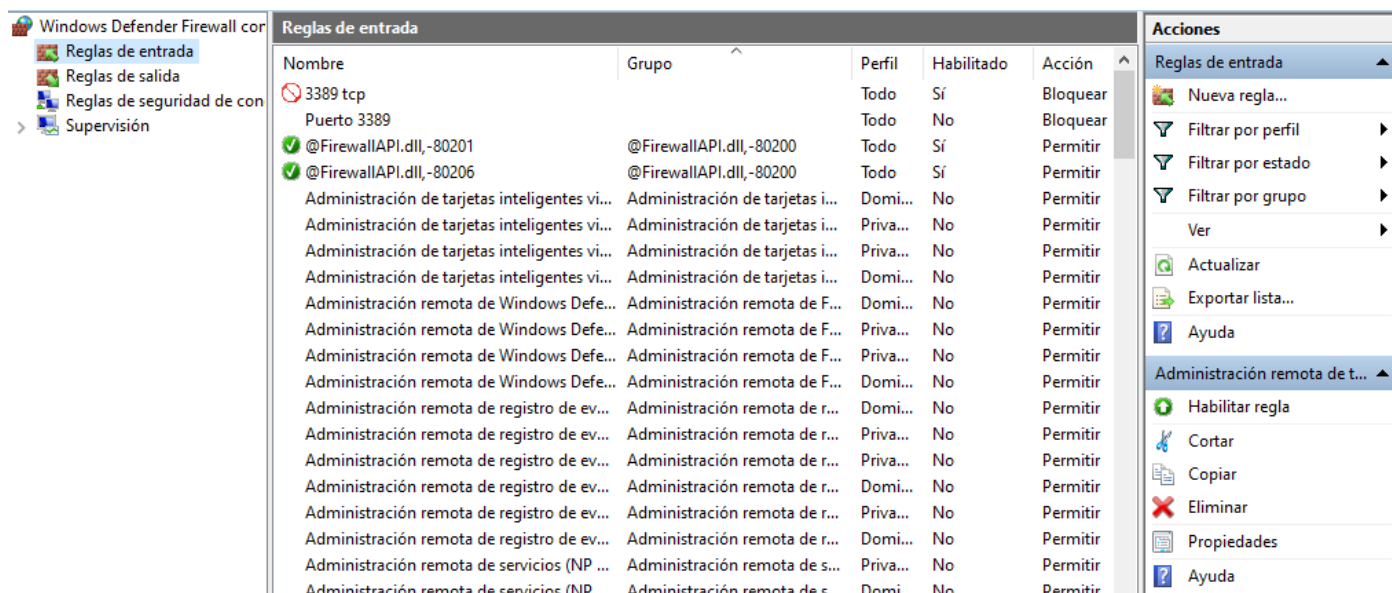


Ilustración 17 Regla de entrada 1

Se iniciará la programa de “Asistente para nueva regla de entrada”

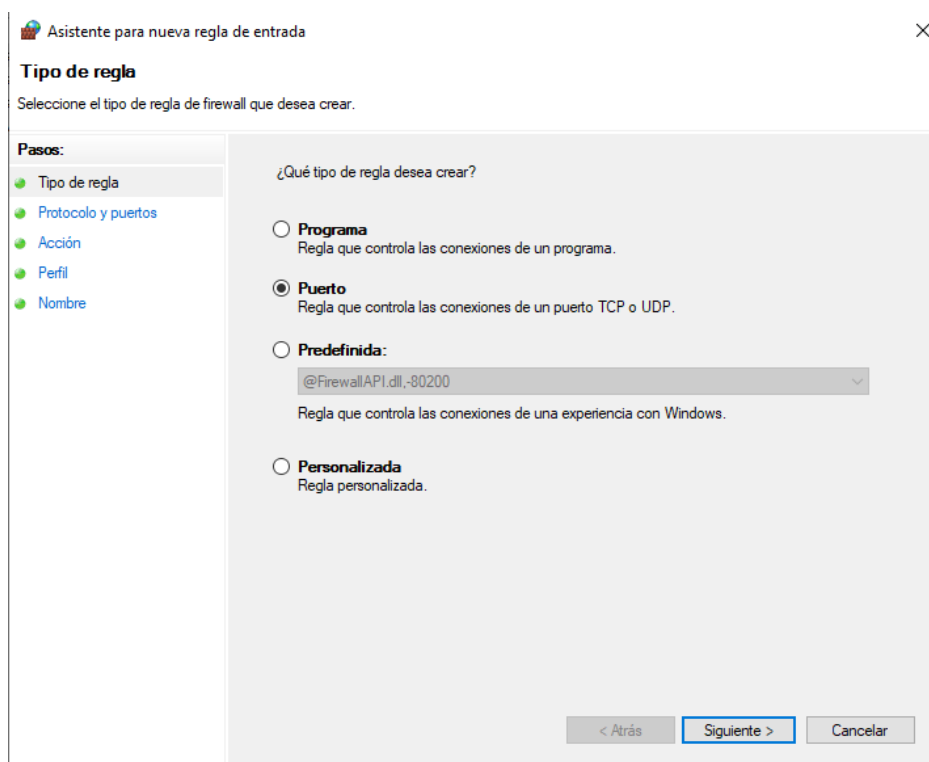


Ilustración 18 Regla de entrada 2

Asistente para nueva regla de entrada

**Protocolo y puertos**

Especifique los puertos y protocolos a los que se aplica esta regla.

**Pasos:**

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

¿Se aplica esta regla a TCP o UDP?

☒ TCP

☐ UDP

¿Se aplica esta regla a todos los puertos locales o a unos puertos locales específicos?

☐ Todos los puertos locales

☒ Puertos locales específicos:

Ejemplo: 80, 443, 5000-5010

< Atrás    Siguiente >    Cancelar

Ilustración 19 Regla de entrada 3

Seleccionamos "Bloquear la conexión"

Asistente para nueva regla de entrada

**Acción**

Especifique la acción que debe llevarse a cabo cuando una conexión coincide con las condiciones especificadas en la regla.

**Pasos:**

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

¿Qué medida debe tomarse si una conexión coincide con las condiciones especificadas?

☐ Permitir la conexión

Esto incluye las conexiones protegidas mediante IPsec y las que no lo están.

☐ Permitir la conexión si es segura

Esto incluye solamente las conexiones autenticadas mediante IPsec. Éstas se protegerán mediante la configuración de reglas y propiedades de IPsec del nodo Regla de seguridad de conexión.

☒ Bloquear la conexión

< Atrás    Siguiente >    Cancelar

Ilustración 20 Regla de entrada 4



Asistente para nueva regla de entrada

**Perfil**

Especifique los perfiles en los que se va a aplicar esta regla.

**Pasos:**

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

¿Cuándo se aplica esta regla?

☒ **Dominio**  
Se aplica cuando un equipo está conectado a su dominio corporativo.

☒ **Privado**  
Se aplica cuando un equipo está conectado a una ubicación de red privada, como una red doméstica o del lugar de trabajo.

☒ **Público**  
Se aplica cuando un equipo está conectado a una ubicación de redes públicas.

< Atrás   Siguiente >   Cancelar

Ilustración 21 Regla de entrada 5

Por ultimo agregamos un nombre y una descripción a la regla y seleccionamos "Finalizar"

Asistente para nueva regla de entrada

**Nombre**

Especifique el nombre y la descripción de esta regla.

**Pasos:**

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

Nombre:  
Puerto 3389

Descripción (opcional):  
Bloquear conexion puerto 3389

< Atrás   Finalizar   Cancelar

Ilustración 22 Regla de entrada 6

FIREWALL	SERVICIO RDP 3389/TCP	nmap UNFILTERED	nmap FILTERED	hping RESPUESTA RESET (R), VOID
Desactivado	Desactivado	<pre> root@kali:~# nmap 192.168.3.5 -p 3389 -sA Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-22 19:06 CET Nmap scan report for 192.168.3.5 Host is up (0.00084s latency).  PORT      STATE      SERVICE 3389/tcp  unfiltered ms-wbt-server  Nmap done: 1 IP address (1 host up) scanned in 13.03 seconds </pre>		<pre> root@kali:~# hping3 192.168.3.5 -p 3389 -A HPING 192.168.3.5 (eth0 192.168.3.5): A set, 40 headers + 0 data bytes len=46 ip=192.168.3.5 ttl=127 DF id=13539 sport=3389 flags=R seq=0 win=0 rt t=8.6 ms len=46 ip=192.168.3.5 ttl=127 DF id=13540 sport=3389 flags=R seq=1 win=0 rt t=7.7 ms len=46 ip=192.168.3.5 ttl=127 DF id=13541 sport=3389 flags=R seq=2 win=0 rt t=6.8 ms ^C --- 192.168.3.5 hping statistic --- 3 packets transmitted, 3 packets received, 0% packet loss round-trip min/avg/max = 6.8/7.7/8.6 ms </pre>
Desactivado	Activado	<pre> root@kali:~# nmap 192.168.3.5 -p 3389 -sA Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-22 19:07 CET Nmap scan report for 192.168.3.5 Host is up (0.00082s latency).  PORT      STATE      SERVICE 3389/tcp  unfiltered ms-wbt-server  Nmap done: 1 IP address (1 host up) scanned in 13.03 seconds </pre>		<pre> root@kali:~# hping3 192.168.3.5 -p 3389 -A HPING 192.168.3.5 (eth0 192.168.3.5): A set, 40 headers + 0 data bytes len=46 ip=192.168.3.5 ttl=127 DF id=13547 sport=3389 flags=R seq=0 win=0 rt t=5.5 ms len=46 ip=192.168.3.5 ttl=127 DF id=13548 sport=3389 flags=R seq=1 win=0 rt t=4.0 ms ^C --- 192.168.3.5 hping statistic --- 2 packets transmitted, 2 packets received, 0% packet loss round-trip min/avg/max = 4.0/4.8/5.5 ms root@kali:~# </pre>
Activado	Desactivado	<pre> root@kali:~# nmap 192.168.3.5 -p 3389 -sA Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-22 19:09 CET Note: Host seems down. If it is really up, but blocking our ping probes, tr y -Pn Nmap done: 1 IP address (0 hosts up) scanned in 3.03 seconds </pre>		<pre> root@kali:~# hping3 192.168.3.5 -p 3389 -A HPING 192.168.3.5 (eth0 192.168.3.5): A set, 40 headers + 0 data bytes ^C --- 192.168.3.5 hping statistic --- 14 packets transmitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms </pre>
Activado	Activado	<pre> root@kali:~# nmap 192.168.3.5 -p 3389 -sA Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-22 19:11 CET Note: Host seems down. If it is really up, but blocking our ping probes, tr y -Pn Nmap done: 1 IP address (0 hosts up) scanned in 3.04 seconds </pre>		<pre> root@kali:~# hping3 192.168.3.5 -p 3389 -A HPING 192.168.3.5 (eth0 192.168.3.5): A set, 40 headers + 0 data bytes ^C --- 192.168.3.5 hping statistic --- 26 packets transmitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms </pre>

4. COMO HABRÁS COMPROBADO POR LAS PRUEBAS REALIZADAS, A TRAVÉS DE LA GENERACIÓN Y ENVÍO DE PAQUETES ACK MAL FORMADOS SE PUEDE LLEGAR A INFERIR LA EXISTENCIA DE UN FIREWALL. CONFIGURA IPTABLES EN EL ROUTER UBUNTU SERVER PARA QUE FILTRE LOS PAQUETES DE TIPO ACK MAL FORMADOS Y NO SE PUEDA REALIZAR EL FINGERPRINTING PARA LA DETECCIÓN DE UN FIREWALL. PARA ELLO PUEDES CONSULTAR LAS "EXTENSIONES TCP" DE LA WEB DE NETFILTER.

Creamos la siguiente regla "iptables -A FORWARD -p tcp --tcp-flags ALL ACK -j DROP"

```
root@planb:~# iptables -A FORWARD -p tcp --tcp-flags ALL ACK -j DROP
root@planb:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp flags:FIN,SYN,RST,PSH,ACK,URG/ACK

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@planb:~#
```

*Ilustración 23 Regla iptables*

Desde Kali insertamos el siguiente comando "nmap 192.168.3.5 -p 3389 -sA" y "hping3 192.168.3.5 -p 3389 -A"

Podemos observar que el resultado que nos da con ambas herramientas es que hay firewall.

```
root@kali:~# nmap 192.168.3.5 -p 3389 -sA
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-22 19:37 CET
Nmap scan report for 192.168.3.5
Host is up (0.00076s latency).

PORT      STATE      SERVICE
3389/tcp  filtered  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
root@kali:~# hping3 192.168.3.5 -p 3389 -A
HPING 192.168.3.5 (eth0 192.168.3.5): A set, 40 headers + 0 data bytes
^C
--- 192.168.3.5 hping statistic ---
134 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

*Ilustración 24 Regla iptables*

En cambio, si activamos también el firewall de la maquina Windows 10 el resultado que obtenemos es que no nos devuelve nada haciéndole creer que la maquina no esta levantada

```
root@kali:~# nmap 192.168.3.5 -p 3389 -sA
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-22 19:21 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.04 seconds
```

Ilustración 25 Regla iptables

```
root@kali:~# hping3 192.168.3.5 -p 3389 -A
HPING 192.168.3.5 (eth0 192.168.3.5): A set, 40 headers + 0 data bytes
^C
--- 192.168.3.5 hping statistic ---
11 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Ilustración 26 Regla iptables

Si hacemos las pruebas con el módulo "state" tenemos tres situaciones:

```
root@planb:~# iptables -A FORWARD -p tcp -m state --state NEW --dport 3389 -j DROP
```

Ilustración 27 Regla de iptables

```
root@kali:~# nmap 192.168.3.5 -p 3389 -sA
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-24 18:59 CET
Nmap scan report for 192.168.3.5
Host is up (0.0011s latency).

PORT      STATE      SERVICE
3389/tcp   filtered   ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
```

Ilustración 28 Resultado de la regla

```
root@planb:~# iptables -A FORWARD -p tcp -m state --state ESTABLISHED --dport 3389 -j DROP
```

```
root@kali:~# nmap 192.168.3.5 -p 3389 -sA
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-24 19:07 CET
Nmap scan report for 192.168.3.5
Host is up (0.00083s latency).

PORT      STATE      SERVICE
3389/tcp   unfiltered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 13.03 seconds
```

```
root@planb:~# iptables -A FORWARD -p tcp -m state --state RELATED --dport 3389 -j DROP
```

```
root@kali:~# nmap 192.168.3.5 -p 3389 -sA
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-24 19:08 CET
Nmap scan report for 192.168.3.5
Host is up (0.0011s latency).

PORT      STATE      SERVICE
3389/tcp   unfiltered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 13.03 seconds
```

Si hacemos una regla en iptables en los paquetes TCP en los que las conexiones que sean nuevas o estén establecidas, sin necesidad de que mire los flags o bits sean aceptados y los demás sean rechazados obtenemos el resultado optimo que es que la herramienta piense que este "down" y así no pueda inferir si tenemos un firewall.

```
root@planb:~# iptables -A FORWARD -p tcp -m state --state NEW,ESTABLISHED --dport 3389 -j ACCEPT
root@planb:~# iptables -A FORWARD -j DROP
```

```
root@kali:~# nmap 192.168.3.5 -p 3389 -sA
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-24 19:05 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.05 seconds
root@kali:~# █
```